**To check Paste, Read and Execute on File Server**

**2.1. File Server**

## **:**

**2.1.1 File Server Setup**

* Login to the MD server.
* Open file explorer.
* Right click on folder which we need to share.
* Popup window will open.
* On that window there will be an option ‘Give access to’, click on that and select give access to specified user/people.
* After entering on Network access window give access to chosen person and mention permissions that you need to give. After that click on share button at bottom right.

**2.1.2 How to check Read, Write and Execute on File Server**

* Open the "File Explorer", in that on Address Bar, enter address of MD server.

e.g. “\\192.168.56.107” and press enter key.

* After pressing enter key, there will be a popup box open which shows shared folder from file server.
* From that window right click on the shared folder, popup box will open, at the end of the popup box click on the Properties.
* In Properties on the upside, there is a "Security" box that will be present. Click on that.
* At the bottom of the "Security" box there will be a "Permission for Authenticated Users" table that will be present.

TS System File Server

Logs

Fig 2.1: File Server Connectivity

**How to create PowerShell script:**

1.Open PowerShell IDE and paste below content into PowerShell:

Function Write-Log

{

[CmdletBinding()]

Param(

[Parameter(Mandatory=$False)]

[ValidateSet("INFO","WARN","ERROR","FATAL","DEBUG")]

[String]

$Level = "INFO",

[Parameter(Mandatory=$True)]

[string]

$Message,

[Parameter(Mandatory=$False)]

[string]

$logfile

)

$content = "[$Stamp] [$Level] $Message"

if($logfile)

{

Add-Content $logfile -Value $content

}

else

{

Write-Output $content

}

}

function Get-CurrentLineNumber

{

$MyInvocation.ScriptLineNumber

}

$ScriptDirectory = "{{cache\_dir}}"

$InstallerLogFileName="$ScriptDirectory\fileserver\_check\_write.txt"

try

{

Copy-Item -Path '{{shared\_dir}}\{{sample\_file\_name}}' -Destination \\{{file\_server\_ip}}\{{file\_server\_shared\_folder}}

Write-Log "INFO" "[$(Get-CurrentLineNumber)] 'File Write successfully.' "$InstallerLogFileName""

}

catch

{

Write-Log "INFO" "[$(Get-CurrentLineNumber)] 'Exception Occur, Can not Write and Execute File.' "$InstallerLogFileName""

}

2.Save the file with ‘FileServer\_Check\_RWX.ps1’

## **Evidence:**

* Local Execution with Evidence
* Login to the TS server.
* Open the "File Explorer”, on address bar enter IP of File Server.

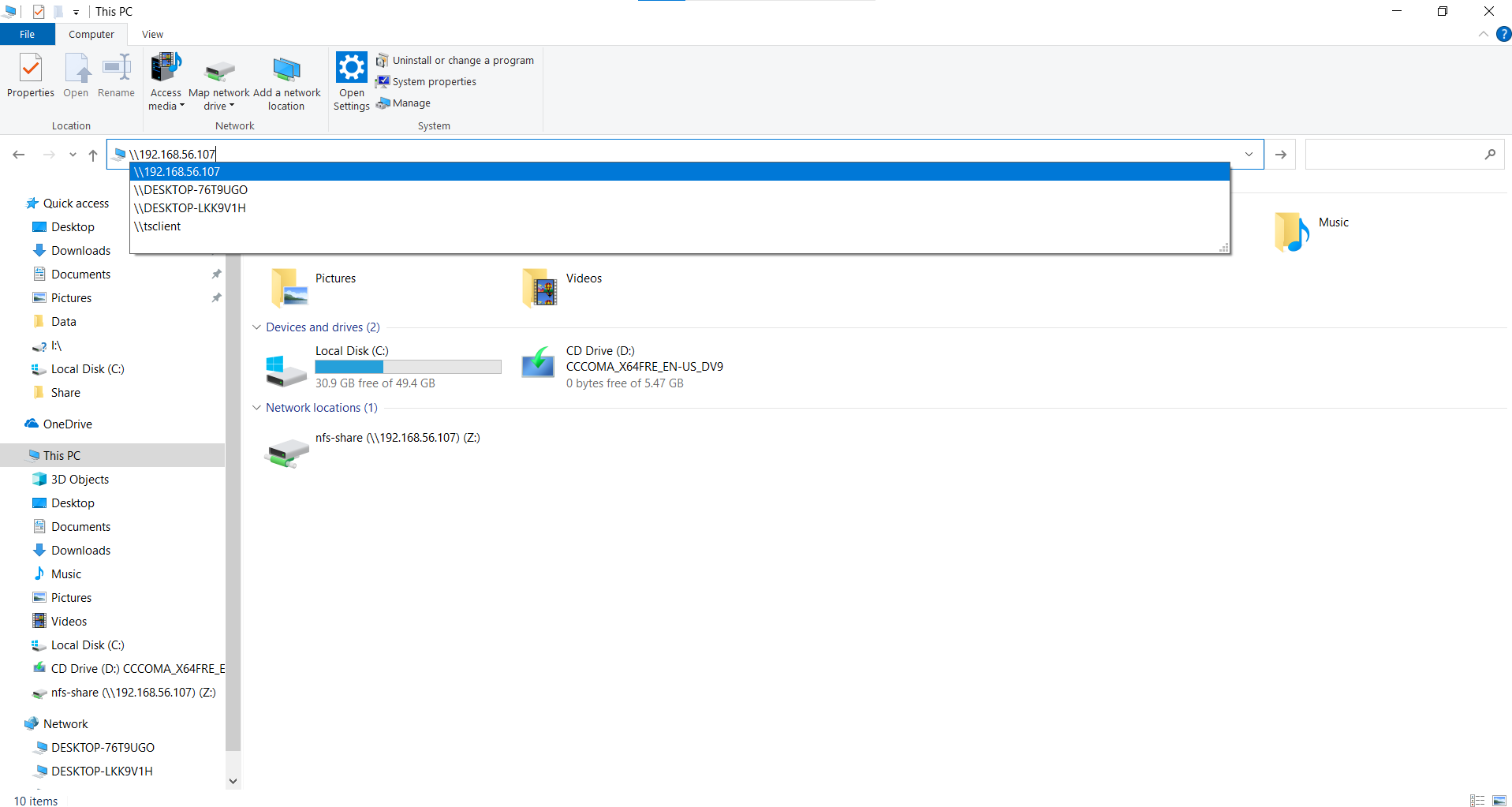


Fig 2.2: Into the File Explorer On address bar

* Press Enter key.
* There will be a popup box of shared file server open.

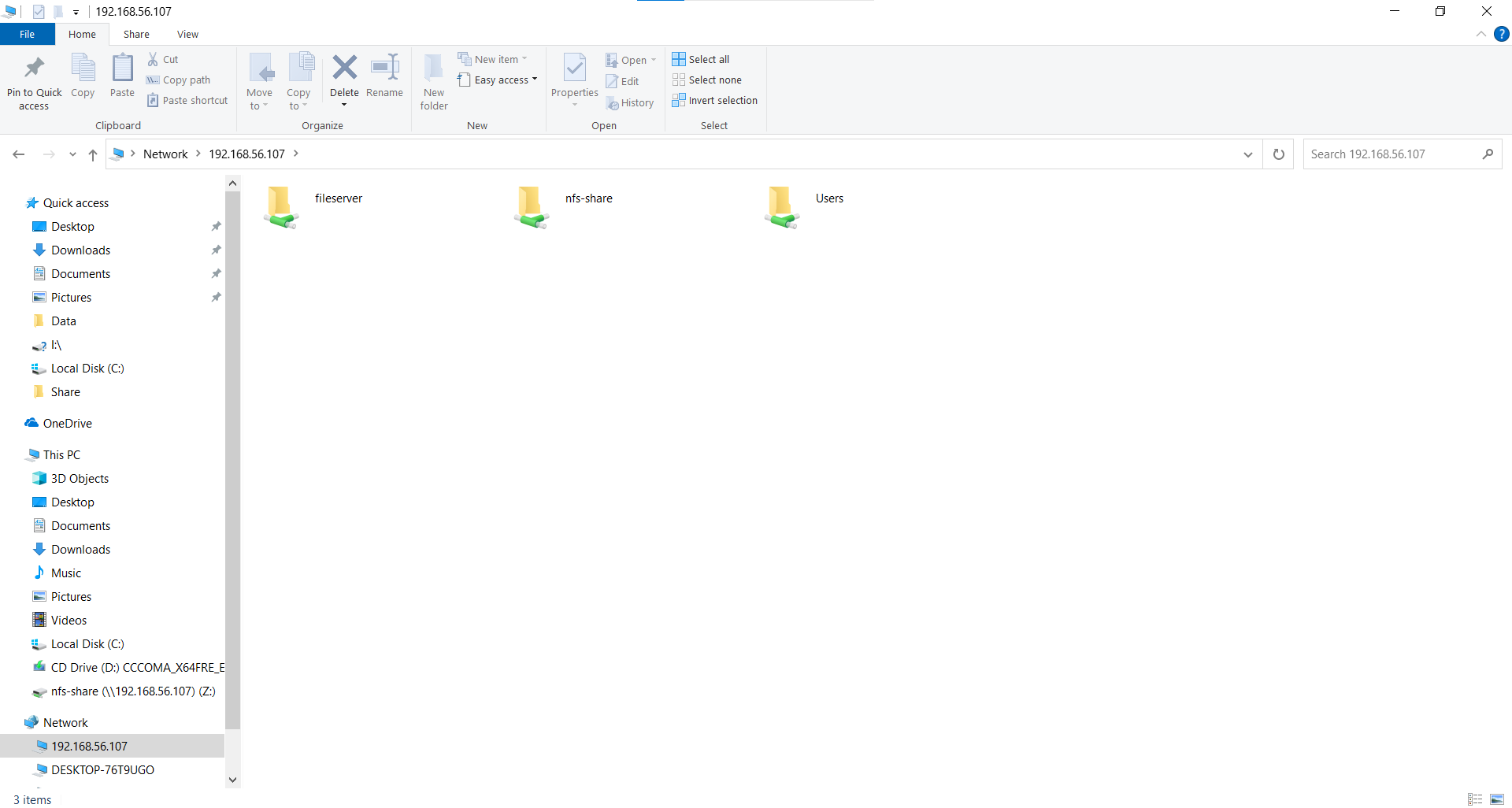


Fig.2.3: After pressing Enter key, popup window of File server

* Select your shared folder & right click on it, at the end of opened popup box, click on the Properties.

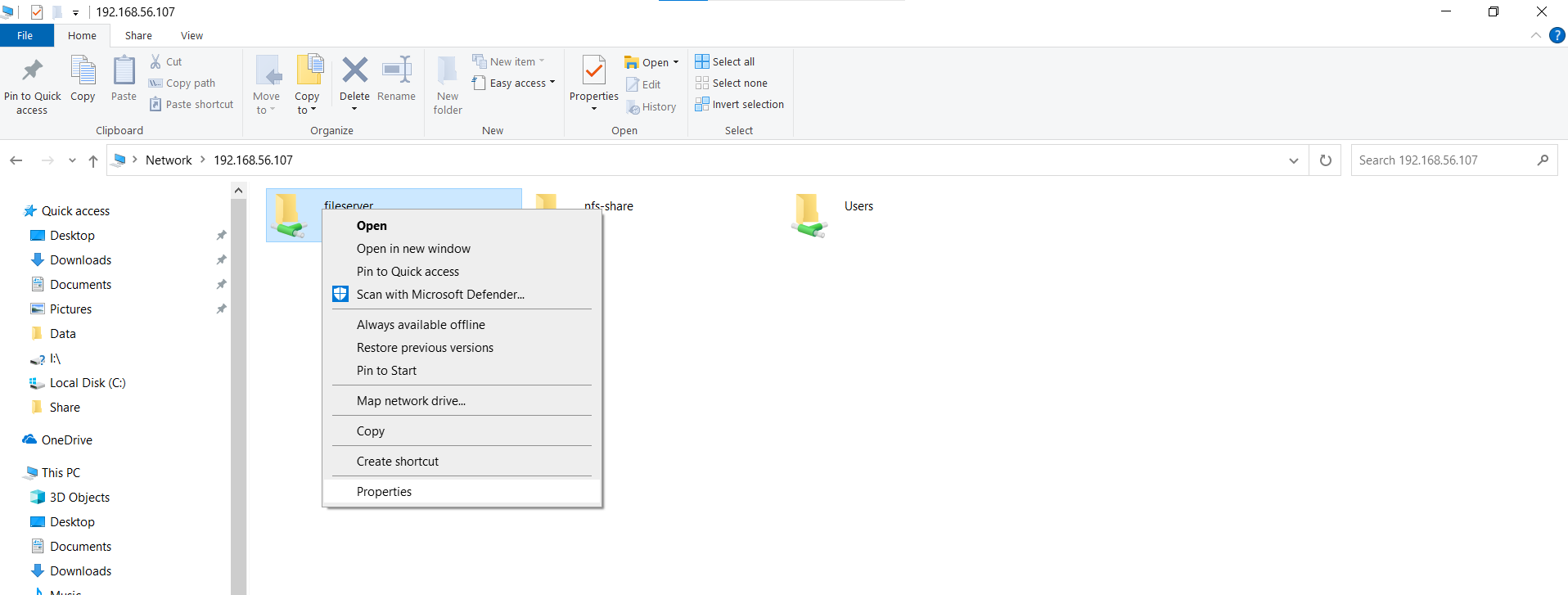


Fig.2.4: Popup box after Right Clicking

* In Properties on the upside, there is a "Security" box that will be present. Click on that.

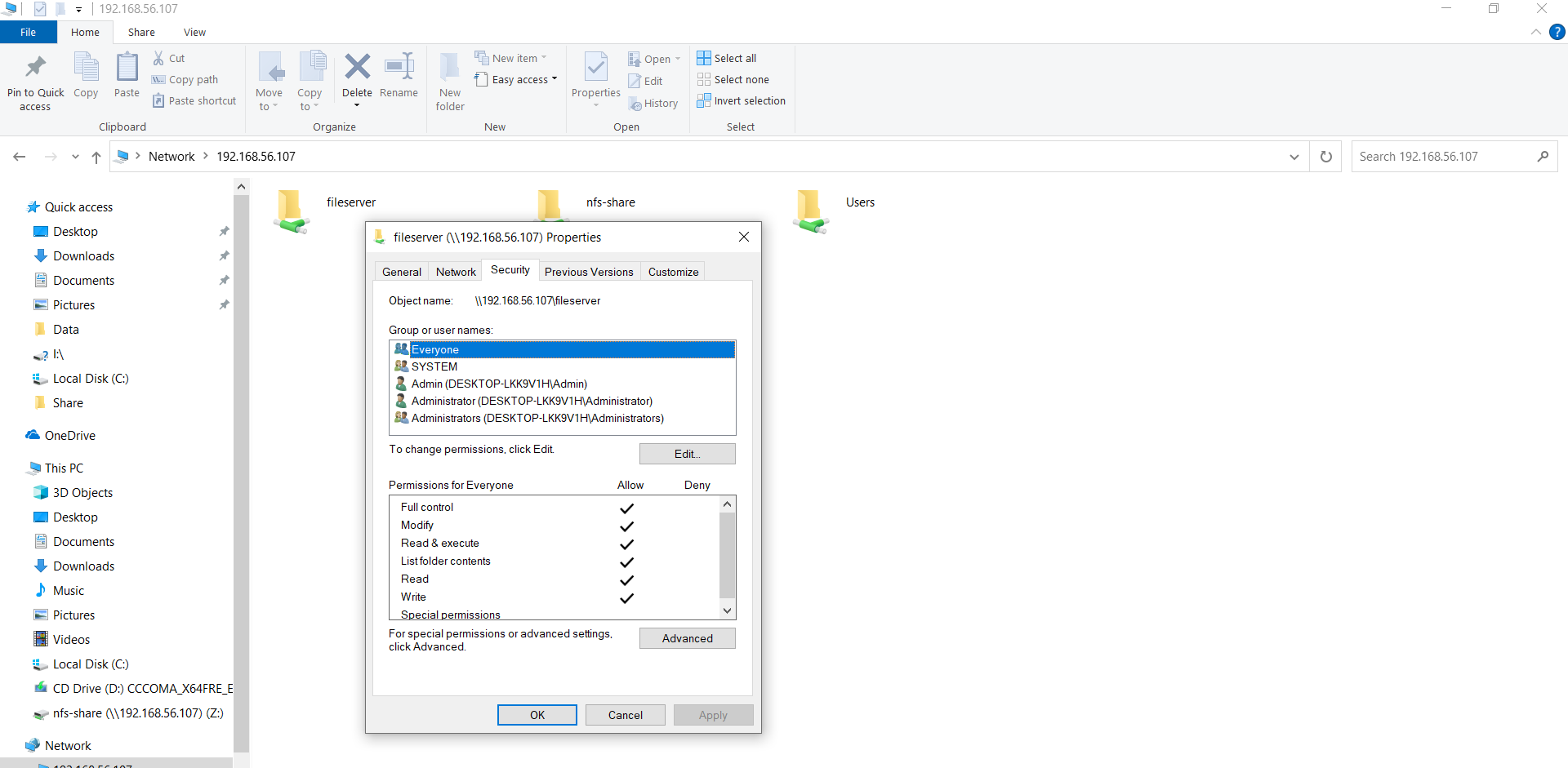


Fig2.5: Window For permission Access

* At the bottom of the "Security" box there will be a "Permission For Authenticated Users" table that will be present.
* To read, write and execute execute below commands on PowerShell.
* To write and execute execute below command:

Syntax:

Copy-Item -Path '<shered\_dir>' -Destination \\<file\_server\_ip>\<file\_server\_shared\_folder>

Example:

Copy-Item -Path 'C:\Share\Sample.ps1' -Destination [\\192.168.56.107\](file:///\\192.168.56.107\oiu)oiu

* To read from file\dir execute below command

Get-Childitem –Path \\<file\_server\_ip>\<file\_server\_shared\_folder>

Example:

Get-Childitem –Path \\<file\_server\_ip>192.168.56.107\oiu

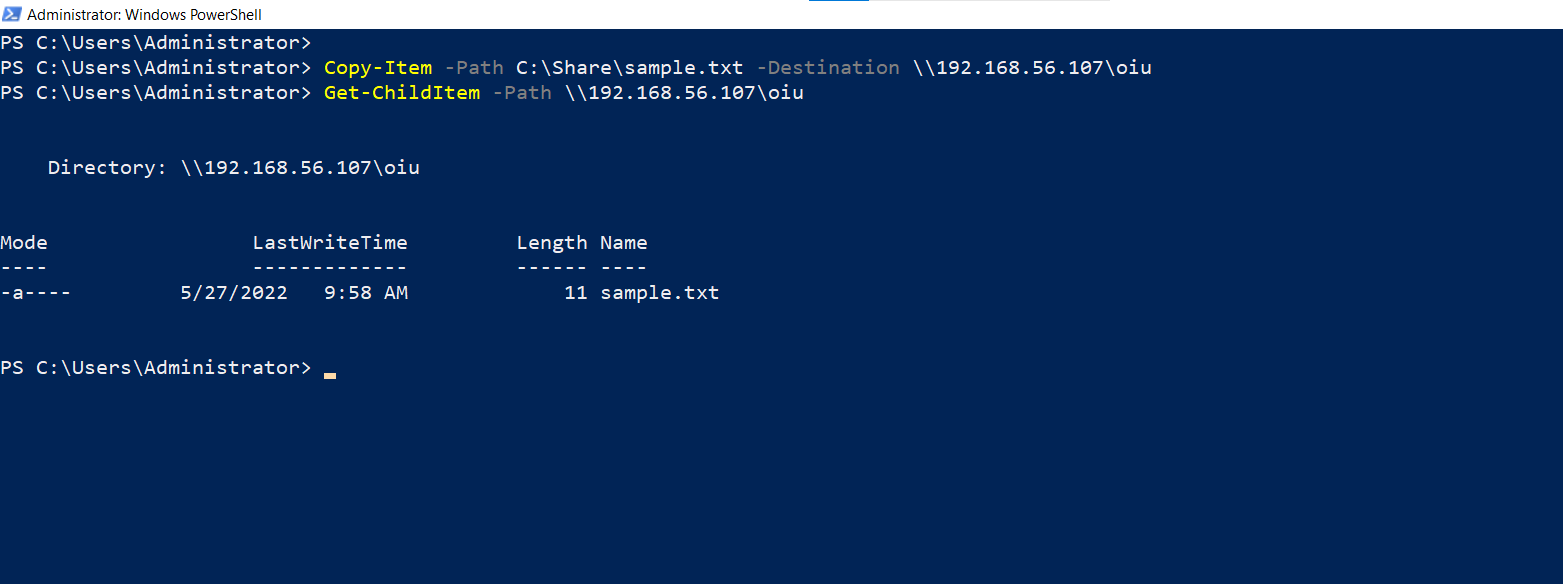


Fig 2.6: Read write and execute on shared file.

* Remote Execution with Evidence

python

import winrm

s = winrm.Session(‘<target\_machine\_ip>’, auth=(‘<user\_name>’,’<password>’))

r = s.run\_ps('C:\\FileServer\_Check\_RWX.ps1')

r.status\_code

In FileServer\_Check\_RWX.ps1 file we are using below commands

To write and execute:

Copy-Item -Path '{{Path\_of\_File\_Dir\_to\_copy\_into\_file\_server}}' -Destination \\{{file\_server\_ip}}\{{file\_server\_shared\_folder}}

To read file:

Get-Childitem –Path \\{{file\_server\_ip}}\{{file\_server\_shared\_folder}} >>C:Share\fileserver\_check\_read

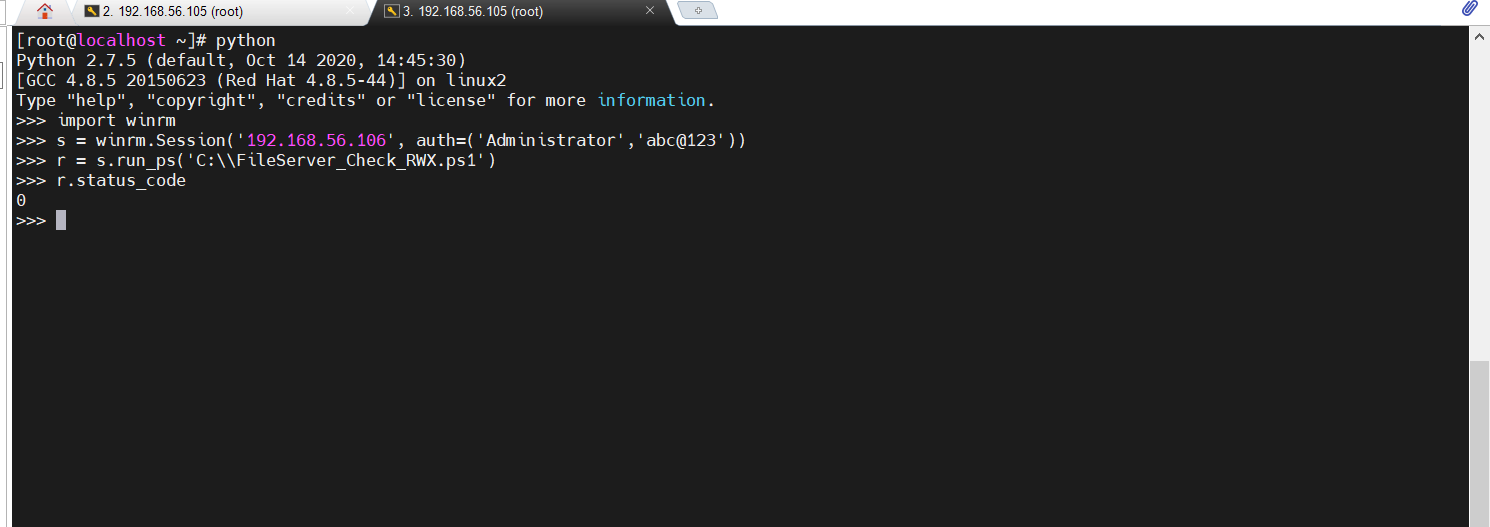


Fig. 2.7: Remote Execution on MD System Successful status evidence

## **Verification:**

* Login TS system.
* Open This PC.
* Go into local disk (C:\).
* Go into Share folder, fileserver\_check\_write\_execute.txt & fileserver\_check\_read.txt must be present.
* Which contain information regarding performed operations.

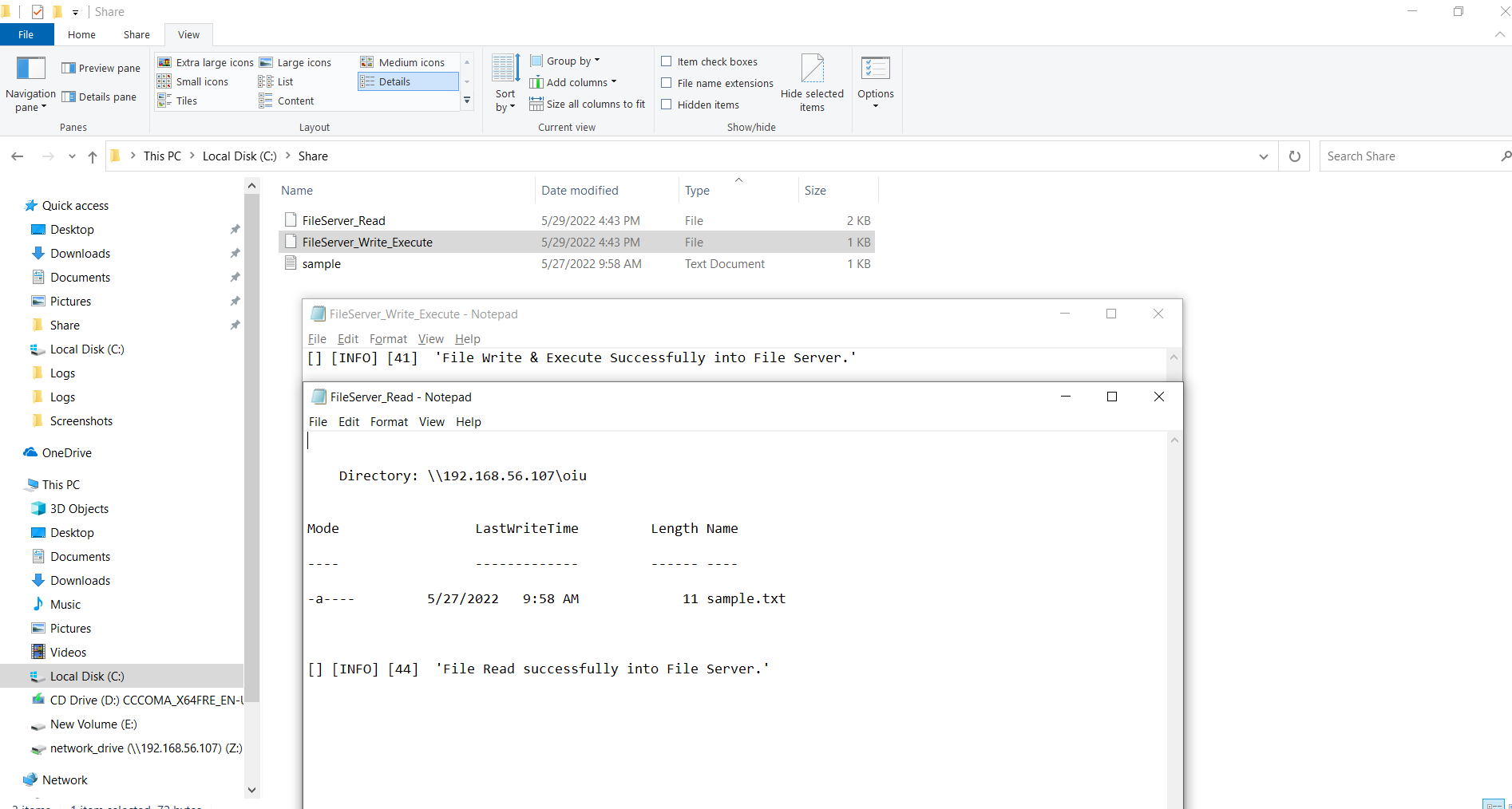


Fig. 2.8: Log generated on MD system after remote execution